



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/840,230	04/24/2001	Stuart Gerald Stubblebine	2455-4230US3	5050

7590
Mr. S H Dworetsky
AT&T Corp
P O Box 4110
Middletown, NJ 07748

08/29/2007

EXAMINER

ZEE, EDWARD

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

08/29/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/840,230

Applicant(s)

STUBBLEBINE, STUART GERALD

Examiner

Edward Zee

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 March 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 52-56 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 52-56 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the request for continued examination filed on March 28th, 2006.

Claims 52-56 are pending and have been considered below.

Response to Amendment

2. The amendment filed on March 28th, 2006 has been considered but is ineffective to overcome the Abadi et al. ("A Semantics for a Logic Authentication", 1991), Denning et al. ("Timestamps in Key Distribution Protocols", 1981) and Van Oorschot et al. (5,699,431) references.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. **Claim 56 is rejected under 35 U.S.C. 102(b) as being anticipated by Abadi et al. ("A Semantics for a Logic Authentication", 1991).**

Claim 56: Abadi et al. discloses a system for system security in a distributed system network comprising:

a. means for preparing a statement(*ie. server responds with message containing a timestamp, the new key and an encrypted submessage*) of an assigned revocation authority(*ie. server*) in a distributed system network in response to a policy(*ie. policy of the system may be to*

Art Unit: 2135

consider messages "fresh" if they are not sent before the start of the current authentication, but not limited to only this constraint), said revocation authority statement being associated with an initial statement(*ie. initial request for a key for A and B by transmitting A's and B's names*) [page 201, column 2];

b. means for preparing a statement of a freshness constraint period(*ie. the time period being the start time of the authentication to the current time, and only timestamps which fall within this period may be considered "fresh"*) in the distributed system network in response to said policy, said freshness statement(*ie. timestamp*) being associated with said revocation authority statement(*ie. timestamp is included in the server's response message*) [page 201, column 2];

c. means for preparing a validity statement at said assigned revocation authority in the distributed system network in response to said policy(*ie. policy may contain the particular keys to use for A and B*), said validity statement including a verification status at some temporal reference(*ie. server encrypts message(containing timestamp, the new keys, etc.) with key K_{as}*) [page 201, column 2];

d. means for providing said revocation authority statement, said freshness statement, and said validity statement to a verification authority in the distributed system network(*ie. B may act as it's own verification authority by decrypting the submessage with key K_{bs} , which is only known to B and S, thus if B can properly decrypt the message then the message is verified*) [page 201, column 2];

e. and means for selectively verifying said initial statement(*ie. A's name*) at said verification authority in response to said initial statement, said revocation authority statement,

Art Unit: 2135

said freshness statement, and said validity statement(*ie. if B successfully decrypts the submessage containing A's name, then the name is verified*) [page 201, column 2].

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abadi et al. ("A Semantics for a Logic Authentication", 1991) in view of Denning et al. ("Timestamps in Key Distribution Protocols", 1981).**

Claim 52: Abadi et al. discloses a method for system security in distributed systems, comprising the steps of:

- a. deriving freshness constraints from initial policy assumptions and an authentic statement [page 201, column 2];
- b. imposing freshness constraints by employing recent-secure authenticating principals to effect revocation [page 201, column 2].

However, Abadi et al. does not explicitly disclose verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

Nonetheless, Denning et al. discloses a similar method and further discloses verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification [page 534, column 2].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to utilize the additional features disclosed by Denning et al. when performing the method disclosed by Abadi et al.. One would have been motivated to do so in order to protect against replay attacks.

Claim 53: Abadi et al. discloses a system for enforcing revocation in distributed systems, comprising:

- a. means for creating time-stamped validity assertion message pertaining to the validity of an initial assertion [page 202, column 1];
- b. means for asserting a freshness constraint indicating a length of time, and relating to said initial assertion [page 204, column 1].

However, Abadi et al. does not explicitly disclose verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

Nonetheless, Denning et al. discloses a similar system and further discloses verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a

Art Unit: 2135

time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification [page 534, column 2].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to utilize the additional features disclosed by Denning et al. within the system disclosed by Abadi et al. One would have been motivated to do so in order to protect against replay attacks.

Claim 54: Abadi et al. discloses a system for protecting an authority of a distinguished principal and enforcing revocation when the authority is compromised, comprising:

- a. a first means for issuing an authoritative assertion by a distinguished principal(*ie. server*) [page 201, column 2];
- b. a second means for asserting freshness constraints on the assertion(*ie. timestamp*) [page 201, column 2];
- c. a third means for asserting a time stamped validity assertion to the assertion indicating the validity of the assertion at the time of the time stamp(*ie. server encrypts message(containing timestamp, the new keys, etc.) with key K_{as}*) [page 201, column 2];

However, Abadi et al. does not explicitly disclose verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

Nonetheless, Denning et al. discloses a similar system and further discloses verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a

Art Unit: 2135

time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification [page 534, column 2].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to utilize the additional features disclosed by Denning et al. within the system disclosed by Abadi et al.. One would have been motivated to do so in order to protect against replay attacks.

7. Claim 55 is rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al. (5,699,431) in view of Denning et al. (“Timestamps in Key Distribution Protocols”, 1981).

Claim 55: Van Oorschot et al. discloses a system for issuing certificates in a system for enforcing revocation in distributed systems, comprising:

- a. means for issuing certificates for principals within an organization by the organization(*ie. certificate authority or other entities*) [column 2, lines 49-62];
- b. means for asserting, by the organization, a principal authorized as an authority(*ie. entities directly or indirectly authorized by the certificate authority for issuing certificates*) for issuing time stamped certificates(*ie. time_and_date_of_issue*) [column 2, lines 49-62 & figure 2];
- c. means for delegating authority(*ie. certificate authority may directly or indirectly authorize entities*) for issuing time stamped certificates [column 2, lines 49-62];
- d. means for asserting freshness constraints(*ie. validity period*) on assertions [column 1, lines 36-39];

However, Abadi et al. does not explicitly disclose verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification.

Nonetheless, Denning et al. discloses a similar system and further discloses verifying that a relation $|t_{now} - t_{timestamp}| \leq \delta$ is satisfied for verification of a secure channel, where $t_{timestamp}$ being a time of a time stamp pertaining to the validity assertion of a particular assertion, δ being a minimum necessary freshness constraint pertaining to the particular assertion and t_{now} being the time of verification [page 534, column 2].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to utilize the additional features disclosed by Denning et al. within the system disclosed by Abadi et al.. One would have been motivated to do so in order to protect against replay attacks.

Response to Arguments

8. Applicant's arguments filed March 28th, 2006 have been fully considered but they are not persuasive.

9. **Regarding Claim 56:**

a. The applicant argues that the “server” is not in “the distributed system network”. However, the Examiner respectfully disagrees and submits that while Abadi et al. does not explicitly disclose the term “distributed system network”, figure 1 shows a network of distributed systems(ie. server and users A and B are connected via at least a

network) and further performing various functions such as key requests, key distributions, authentication and verification across the network.

b. The Applicant argues that a “freshness constraint period” is not specified.

However, the Examiner respectfully disagrees and submits that Abadi et al. does in fact disclose a “freshness constraint period”, the time period being the start time of the authentication to the current time, and only timestamps which fall within this period may be considered “fresh”.

c. The Applicant argues that the message the “server” sends is not in response to the previously identified policy, not associated with a revocation authority statement and that no policy exists. However, the Examiner respectfully disagrees and submits that while Abadi et al. does not explicitly disclose the term “policy”, a policy is in fact employed, wherein the policy of the system may be to consider messages “fresh” if they are not sent before the start of the current authentication. Furthermore, since the revocation authority(ie. “server”) is preparing this “statement”, it is in fact associated with the revocation authority and sent from the revocation authority as well.

d. The Applicant argues that no “validity statement” is verified. However, the Examiner respectfully disagrees and submits that if a message is encrypted with a key only known to two individuals, the individual decrypting the message can “verify” the message if the message is properly decrypted with the key.

10. Regarding Claim 52:

a. The Applicant argues that Abadi et al. merely discloses a time, and does not provide a threshold of what is considered fresh. The Examiner respectfully disagrees and

would like to first refer back to Applicant's statement regarding freshness. The Applicant states that *"the date this item came into being is May 2005 tells nothing about whether the item is fresh"* and that *"only if another time is specified so that the age can be ascertained, and some other information is known that relates to what is considered fresh"*, and lastly *"it is essential to one to KNOW that now is November 2005"*. The Examiner would like to use the milk item example as proposed by the Applicant. A standard container of milk will have a timestamp("the date this item came into being") and an expiration date(freshness policy). Most people would be able to successfully determine the freshness of the milk by analysis these two constraints provided on the container. Furthermore it would be unfeasible to attempt to provide a "current time"(the time that the freshness is checked) timestamp, such as providing one on the milk container, which appears to be what the Applicant suggests, is lacking regarding the Abadi et al. reference. Thus, one can in fact determine the freshness of a message by providing a timestamp and knowing the policy as Abadi et al. has disclosed.

b. The Applicant argues that the freshness constraint disclosed by Abadi et al. is preordained as opposed to being derived. However, the Examiner respectfully disagrees and submits that one can consider the freshness constraint as being derived from the freshness policy, as one must first discover(or "derive") what is considered fresh by referring to the freshness policy, before one knows how to determine freshness.

c. The Applicant argues that Abadi et al. does not disclose "imposing freshness constraints by employing recent-secure authenticating principals to effect revocation". However, the Examiner respectfully disagrees and submits that Abadi et al. states that

messages are considered “fresh” if they are not sent before the start of the current authentication, which in turn is a freshness constraint.

d. The Applicant argues that Denning et al. does not disclose “a minimum necessary freshness constraint pertaining to the particular assertion”. However, the Examiner respectfully disagrees and submits that the “less than one or two minutes” disclosed by Denning et al. is in fact a form of a freshness constraint(ie. time limitation).

11. Regarding Claim 53:

a. The Applicant argues that the time stamped message created by the server does not say anything about the validity of the message. However, the Examiner respectfully disagrees and submits that if a message is encrypted with a key only known to two individuals, the individual decrypting the message can establish that the message is valid if the message is properly decrypted with the key, and furthermore the individual can establish that the identification(ie. A, B) encrypted in the message is valid as well.

b. The Applicant argues that Abadi et al. does not describe a freshness constraint, which indicates a length of time, and that it does not relate to the initial assertion. However, the Examiner respectfully disagrees and submits that a length of time is in fact disclosed, that length of time being the start time of the authentication to the current time, and only timestamps which fall within this period, may be considered “fresh”. Furthermore, the freshness constraint(ie. timestamp) is also appended to the identification(ie. A, B), which signifies that the freshness constraint is in fact related to the initial assertion.

c. The Applicant argues the teachings of Denning et al., which has been addressed above.

12. Regarding Claim 54:

a. In response to applicant's arguments, the recitation "for protecting an authority of a distinguished principal and enforcing revocation when the authority is comprised" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

b. The Applicant argues the teachings of Denning et al., which has been addressed above.

13. Regarding Claim 55:

a. The Applicant argues that there is no teaching or suggestion of a means for asserting a principal that is authorized as an authority, or a means for delegating authority. However, the Examiner respectfully disagrees and submits that Van Oorschot et al. does in fact disclose this in column 2, lines 49-62 of the reference(ie. "other entities directly or indirectly authorized by the certification authority for digitally issuing a certificate"), wherein the "other entities" may be viewed as a "principal" and the "certification authority" may be viewed as the "delegating authority".

Art Unit: 2135

b. The Applicant argues the teachings of Denning et al., which has been addressed above.

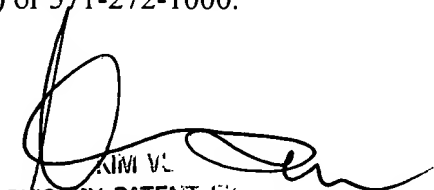
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
August 21, 2007


KIM Y. VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100